**программный продукт**

**«Professional Identity Security Manager»**

**«PRISMA»**

**Руководство пользователя**

**АННОТАЦИЯ**

Данное руководство содержит описание изделия «Professional Identity Security Manager», (далее – Prisma, изделие) и предназначено для пользователей Prisma. Руководство пользователя включает:

* сведения о назначении Prisma и информацию, достаточную для понимания функций Prisma и его эксплуатации;
* описание условий, необходимых для выполнения программы (минимальный состав аппаратных и программных средств и т.п.);
* условия запуска и завершения работы Prisma;
* описание условий безопасной эксплуатации Prisma;
* описание функций и интерфейсов функций Prisma, доступных каждой роли пользователей;
* описание параметров (настроек) безопасности Prisma, доступных каждой роли пользователей, и их безопасных значений;
* описание типов событий безопасности, связанных с доступными пользователю функциями Prisma;
* информацию по действиям после сбоев и ошибок в эксплуатации Prisma.

СОДЕРЖАНИЕ

[1 НАЗНАЧЕНИЕ PRISMA 7](#_Toc117498086)

[1.1 Состав Prisma 7](#_Toc117498087)

[2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ 8](#_Toc117498088)

[2.1 Требования к авторизации 8](#_Toc117498089)

[2.2 Требования к рабочему месту пользователя 8](#_Toc117498090)

[2.3 Требования к квалификации пользователя 8](#_Toc117498091)

[3 РАБОТА С СИСТЕМОЙ 9](#_Toc117498092)

[**3.1** Подключение и настройка информационных систем (SSO) 9](#_Toc117498093)

[**3.1.1** Создание новой области ИС 9](#_Toc117498094)

[**3.1.2** Настройки Области ИС 9](#_Toc117498095)

[**3.1.3** Удаление области ИС 10](#_Toc117498096)

[**3.1.4** Создание нового клиента 11](#_Toc117498097)

[**3.1.5** Учетные данные клиента 11](#_Toc117498098)

[**3.1.6** Удаление клиента 12](#_Toc117498099)

[**3.2** Взаимодействие с внешними Клиентами 12](#_Toc117498100)

[**3.2.1** Проверка изменений в назначенных пользователю разрешениях (Смена версии токена) 12](#_Toc117498101)

[**3.3** Аутентификация 13](#_Toc117498102)

[**3.3.1** Формирование и выдача токена пользователя 13](#_Toc117498103)

[**3.3.2** Расширения функционала токенов 13](#_Toc117498104)

[**3.3.3** Настройки обязательных действий при аутентификации 15](#_Toc117498105)

[**3.3.4** Подтверждение e-mail при первом входе в УЗ 16](#_Toc117498106)

[**3.4** Аутентификация через Федерации 17](#_Toc117498107)

[**3.4.1** Просмотр списка настроенных каталогов для Федераций пользователей 17](#_Toc117498108)

[**3.4.2** Настройка соединения с Каталогом по LDAP 17](#_Toc117498109)

[**3.4.3** Настройка алгоритмов синхронизации пользователей с Каталогом по LDAP 17](#_Toc117498110)

[**3.4.4** Управление пользователями 18](#_Toc117498111)

[**3.4.5** Настройка соединения с Каталогом по KERBEROS 19](#_Toc117498112)

[3.5 Аутентификация через провайдеров 19](#_Toc117498113)

[**3.6** Управление учетными записями 19](#_Toc117498114)

[**3.6.1** Просмотр списка учетных записей 19](#_Toc117498115)

[**3.6.2** Создание новых пользователей 20](#_Toc117498116)

[**3.6.3** Редактирование учетной записи пользователя 20](#_Toc117498117)

[**3.6.4** Блокировки пользователей 20](#_Toc117498118)

[**3.6.5** Блокирование пользователей вручную 21](#_Toc117498119)

[**3.6.6** Блокировка\активация учетной записи при превышении максимального количества неудачных попыток входа 21](#_Toc117498120)

[**3.6.7** Удаление пользователей 22](#_Toc117498121)

[**3.6.8** Настройки входа 22](#_Toc117498122)

[**3.6.9** Изменение логина после создания учетной записи (УЗ) 23](#_Toc117498123)

[3.6.10 Работа с паролями 23](#_Toc117498124)

[3.7 Управление доступом 24](#_Toc117498125)

[3.7.1 Проверка наличия и выдача требуемых прав пользователям 24](#_Toc117498126)

[**3.7.2** Управление областями видимости 24](#_Toc117498127)

[3.7.3 Управление ролями 26](#_Toc117498128)

[**3.7.4** Управление группами пользователей 28](#_Toc117498129)

[3.7.5 Переход к настройкам авторизации клиента 32](#_Toc117498130)

[**3.7.6** Управление разрешениями 32](#_Toc117498131)

[**3.7.7** Настройки авторизации клиента 34](#_Toc117498132)

[**3.8** Управление сессиями 35](#_Toc117498133)

[**3.8.1** Просмотр, фильтрация и сортировка списка активных сессий для ИС или ее части 35](#_Toc117498134)

[**3.8.2** Просмотр списка оффлайн сессий пользователей в Области ИС 35](#_Toc117498135)

[**3.8.3** Ограничение числа параллельных сессий 36](#_Toc117498136)

[**3.8.4** Завершение сессий администратором подключенной ИС 36](#_Toc117498137)

[**3.8.5** Автоматическое принудительное закрытие сессий по таймауту 36](#_Toc117498138)

[**3.8.6** Завершение собственных сессий субъектом доступа 36](#_Toc117498139)

[**3.9** Журналирование и контроль изменений 37](#_Toc117498140)

[**3.9.1** Настройки регистрации событий безопасности 37](#_Toc117498141)

[**3.9.2** Журналирование событий входа и выхода пользователей 37](#_Toc117498142)

[**3.9.3** Журналирование действий администраторов 37](#_Toc117498143)

[**3.9.4** Ограничение времени хранения событий безопасности 38](#_Toc117498144)

[**3.9.5** Очистка событий безопасности вручную 38](#_Toc117498145)

[**3.9.6** Трансляция событий в syslog 38](#_Toc117498146)

[**3.9.7** Уведомления при критических сбоях в механизмах сбора информации 38](#_Toc117498147)

[**3.9.8** Автоматическая рассылка уведомлений об изменении администраторами прав пользователей 39](#_Toc117498148)

[**3.9.9** Рассылка уведомлений при заполнении объема памяти 39](#_Toc117498149)

[**3.9.10** Рассылка уведомлений о критическом сбое 39](#_Toc117498150)

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 40](#_Toc117498151)

[ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ 41](#_Toc117498152)

# НАЗНАЧЕНИЕ PRISMA

## Состав Prisma

Prisma представляет собой веб-приложение.

При входе в подключенную ИС пользователи перенаправляются на интерфейс аутентификации Prisma.

Далее осуществляется перенаправление пользователя в подключенную ИС.

Общая схема архитектуры Prisma представлена ниже.



**Схема 1 Общая схема архитектуры Prisma**

# УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

## Требования к авторизации

Для взаимодействия внутреннего пользователя Prisma необходимо иметь логин и пароль условно-постоянного действия, а также подтвержденную электронную почту.

Для взаимодействия внешнего пользователя Prisma необходимо иметь логин и пароль условно-постоянного действия, а также подтвержденную электронную почту в случае, если указана необходимость применять МФА для аутентификации.

## Требования к рабочему месту пользователя

Требования к интернет-браузерам для работы в Prisma:

* Google Chrome 40 и выше;
* Mozilla Firefox 36 и выше.

Дополнительное программное обеспечение не требуется.

## Требования к квалификации пользователя

Пользователь должен обладать квалификацией, обеспечивающей, как минимум:

* базовые навыки работы на персональном компьютере с графическим пользовательским интерфейсом (клавиатура, мышь, управление окнами и приложениями, файловая система);
* базовые навыки использования стандартной клиентской программы (см. раздел 2.2).

# РАБОТА С СИСТЕМОЙ

## Подключение и настройка информационных систем (SSO)

### Создание новой области ИС

В случае, если область Информационных систем, в которую необходимо добавить новую ИС, еще не создана, выполняется создание новой области информационных систем. Новую Область ИС можно создать только если авторизоваться под пользователем с правами Супер Администратора. После входа в Prisma необходимо нажать на кнопку создания новой Области ИС.



Рисунок 1 Создание новой области ИС

Далее в открывшемся окне ввести название новой Области ИС и нажать на кнопку «Создать». Область ИС можно включить или выключить при создании. Пользователи и клиенты смогут получить доступ к созданной Области ИС, только если она включена.

### Настройки Области ИС

#### Настройка SMTP-сервера(E-mail)

В Prisma пользователям отправляются электронные письма для:

* подтверждения адреса электронной почты;
* для уведомления администратора о событиях безопасности;
* получения пользователями кодов МФА.

Чтобы включить отправку электронных писем, необходимо настроить параметры SMTP-сервера. Параметры SMTP-сервера настраиваются для Prisma и каждой области ИС отдельно. Для этого необходимо перейти в параметры Области ИС и открыть вкладку «E-mail».

#### Основные настройки

После выбора Области ИС, с которой будет вестись работа, происходит переход на вкладку с настройками данной Области ИС.



Рисунок 2 Основные настройки Области ИС

### Удаление области ИС

В процессе взаимодействия с Prisma, возможна ситуация, когда потребуется перенести все настройки в другую Область ИС. После переноса настроек, ненужную Область ИС стоит удалить.

Перед удалением Области ИС стоит убедиться, что сохранены все требуемые настройки, так как после удаления Области ИС все данные Области ИС полностью удаляются.

Для удаления Области ИС необходимо перейти в настройки Области ИС, нажать на значок удаления Области ИС (корзинка, рядом с названием области ИС) и подтвердить свое действие.=

###  Создание нового клиента

Для создания нового клиента пользователю необходимо:

На [странице просмотра списка клиентов](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131046323) нажать на кнопку «+ Клиент».



Рисунок 3 Кнопка добавления нового клиента «+ Клиент»

Далее появится всплывающее окно «Добавить клиента», в котором необходимо заполнить следующие поля:

* ID клиента\* - обязательное поле для заполнения. Поле задает идентификатор, указываемый в URL и в токенах. Например «my-client». Для SAML это также ожидаемое имя издателя для запросов аутентификации;
* Корневой URL - добавляется к относительным URL.

### Учетные данные клиента

Для просмотра учетных данных клиента пользователю необходимо:

1. Через [страницу просмотра списка клиентов](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131046323) перейти в настройки необходимого клиента.
2. Далее перейти на вкладку «Учетные данные» на рабочей панели, рядом со вкладкой «Настройки».

Перед пользователем появится страница с несколькими полями для заполнения.

### Удаление клиента

В процессе взаимодействия с Prisma, возможна ситуация в который понадобится удалить клиента. Как пример, при случайном создании, или изменении политик настройки авторизации пользователей или прочих действиях.

Для удаления Клиента необходимо выбрать функцию удаления в карточке клиента либо в списке клиентов области ИС.

## Взаимодействие с внешними Клиентами

### Проверка изменений в назначенных пользователю разрешениях (Смена версии токена)

Prisma выпускает новую версию токена при срабатывании событий-триггеров, которые влияют на права подключенных к ИС пользователей, чтобы подключенная ИС могла своевременно получить актуальный набор прав пользователя.

Условие срабатывает при выполнении внутренним пользователем определенных действий.

## Аутентификация

### Формирование и выдача токена пользователя

Для формирования и выдачи токена пользователя необходимо выполнить запрос по API.

### Расширения функционала токенов

####  Аутентификация по логину и паролю

Пользователь переходит по ссылке приложения.
Приложение переадресует пользователя на аутентификации Prisma.
После перехода открывается страница авторизации, где необходимо ввести логин пользователя в поле «Имя пользователя» и пароль пользователя в поле «Пароль».

В результате корректного ввода логина и пароля откроется запрашиваемая страница информационной системы.

#### Аутентификация по базовой схеме HTTP с использованием комбинации пароля и OTP

Для выполнения аутентификации с использованием OTP необходимо в разделе [Требуемые действия](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131053286) 🡪 Аутентификации администратору активировать действие «Привязать мобильное устройство (для одноразового пароля)» (Configure OTP).

Далее пользователю необходимо:

1. Авторизоваться в своей Области ИС;
2. Настроить мобильный аутентификатор по инструкции, представленной на слайде ниже (см. рис);
3. Нажать на кнопку «Отправить»;
4. При корректном вводе кода аутентификатора - выйти из профиля.

#### Двухфакторная аутентификация по дополнительному коду в эл. почте

Двухфакторная аутентификация выполняется следующим образом:

1. Пользователь переходит по ссылке приложения.
2. Приложение переадресует пользователя на аутентификацию Prisma.
3. После успешного ввода логина и пароля, пользователю отправляется электронное письмо с временным кодом и параллельно открывается форма для ввода этого пароля.
4. Пользователь вводит временный код. И в случае успешного ввода, проходит аутентификацию. Далее происходит переадресация на запрашиваемую страницу подключенной ИС.

#### Аутентификация по логину, паролю и recaptcha

Для аутентификации по логину, паролю и recaptcha прежде всего администратору необходимо:

1. Включить по API тумблер «Самостоятельная регистрация пользователей»;
2. В разделе «Аутентификация» на вкладке «[Сценарии входа](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131057594)» выбрать сценарий «Регистрация»;
3. Для действия «Recaptcha» установить требование «Требуется»;
4. Для действия «Recaptcha» [настроить конфигурацию](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131064052).

Далее пользователю необходимо:

1. Перейти на страницу авторизации;
2. Нажать на кнопку «Зарегистрироваться»;
3. После заполнения форм регистрации нажать на кнопку «Я не робот» в окне исполнения «recaptcha».

#### Настройка времени на выполнение аутентификации в Prisma или подключенной ИС

Для того, чтобы настроить время на выполнение аутентификации в Prisma, необходимо перейти в раздел «Настройки Области ИС» далее открыть вкладку «Токены».

На открывшейся странице необходимо установить значение в строках:

* Таймаут входа - максимальное время пользователя, необходимое для входа в систему.
* Таймаут действий по входу - максимальное время, за которое пользователь должен выполнить и завершить действие после входа.

### Настройки обязательных действий при аутентификации

Для перехода на страницу пользователю необходимо:

1. Перейти в раздел Аутентификация;
2. Далее на рабочей панели ниже открыть вкладку «Требуемые действия».

На странице отобразится список со всеми требуемыми действиями при аутентификации.



Рисунок 2 Список требуемых действий

На странице требуемых действий пользователь может:

1. Изменить приоритет требуемого действия;
2. Включить и отключить требуемое действие;
3. Перевести требуемое действие в статус действия по умолчанию

### Подтверждение e-mail при первом входе в УЗ

Для подтверждения e-mail при первом входе в УЗ прежде всего в разделе [Требуемые действия](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131053286) Аутентификации администратору необходимо активировать действие «Верифицировать e-mail» (Verify E-mail).

В результате корректного ввода пароля, полученного на эл. почту, откроется запрашиваемая страница информационной системы.

В случае неполучения одноразового кода пользователь может воспользоваться подсвеченной кнопкой «Нажмите здесь» для повторного запроса электронного письма с кодом.

## Аутентификация через Федерации

###  Просмотр списка настроенных каталогов для Федераций пользователей

Для перехода к странице Федерации пользователей необходимо открыть раздел **Федерации** на рабочей панели слева.

Откроется список с имеющимися настроенными каталогами федерации пользователей.

###  Настройка соединения с Каталогом по LDAP

Для того чтобы перенести данные пользователей в федерации пользователей LDAP в Prisma, в первую очередь необходимо создать новую запись в федерации пользователей, которая будет соответствовать существующей федерации пользователей. Для этого пользователю необходимо:

1. Перейти в раздел Федерации пользователей;
2. Нажать на кнопку «Добавить каталог».

Перед пользователем откроется страница добавления нового каталога, где необходимо отредактировать поля подраздела настроек.

### Настройка алгоритмов синхронизации пользователей с Каталогом по LDAP

Для того чтобы пользователи правильно загрузились, а именно использовались нужные атрибуты и записывались в соответствующих полях базы данных Prisma, необходимо сопоставить их. По умолчанию создаются сопоставления, в которых указаны стандартные параметры приложений LDAP (в зависимости от указанного типа приложения).

### Управление пользователями

#### Загрузка пользователей

Следующим шагом необходимо импортировать пользователей. Для первого импорта необходимо вручную выполнить запрос «Синхронизация всех пользователей»

Далее, чтобы держать актуальные данные в обоих приложениях, рекомендуется настроить периодическую автоматическую синхронизацию, для этого необходимо передать соответствующие параметры в запросе на «Обновление компонента»

#### Поддержка актуальных данных о пользователях

Поддержка актуальных данных пользователей предусматривает полную синхронизацию и синхронизацию только измененных пользователей. При этом, в зависимости от типа хранения пользователей в Prisma, данные могут иметь разное направление, как из Prisma в Приложение LDAP так и из LDAP в Prisma.

Для полной синхронизации необходимо выполнить тот же запрос, что и при загрузке пользователей.

#### Удаление импортированных пользователей

Для удаления импортированных пользователей необходимо выполнить запрос «удаления импортированных пользователей» Отвязка пользователей от федерации пользователей.

Пользователи могут быть отвязаны только все вместе. Одиночная отвязка не возможна.

### Настройка соединения с Каталогом по KERBEROS

Prisma позволяет выполнять аутентификацию пользователей через их интеграцию с каталогами пользователей по протоколу LDAP.
Поддерживается также аутентификация по протоколу Kerberos. Настройка Kerberos выполняется через API. При необходимости его использования следует обратиться к Производителю за соответствующей документацией.

## Аутентификация через провайдеров

В Prisma возможна аутентификация через внешних провайдеров с помощью следующих протоколов:

* SAML v2.0;
* OIDC;
* а также, через социальные сети в качестве поставщика аутентификации (в т.ч. GitHub; GitLab; Facebook; Google; LinkedIn; Microsoft; BitBucket; Twitter; Openshift v3; Openshift v4; PayPal; StackOverflow.

## Управление учетными записями

###  Просмотр списка учетных записей

Чтобы просмотреть список пользователей необходимо открыть пункт меню «**Пользователи**».

### Создание новых пользователей

Для того чтобы создать пользователя, необходимо перейти в раздел пользователи и нажать на кнопку «**+Пользователь**» в правой части экрана.



Рисунок 5 Кнопка создания пользователей

В результате нажатия на кнопку откроется Модальное окно, с формой создания нового пользователя.

### Редактирование учетной записи пользователя

Для того, чтобы отредактировать учетную запись пользователя, необходимо в этом же разделе нажать на кнопку «**Редактировать**» напротив нужной строки или нажать на строку с необходимым пользователем.

### Блокировки пользователей

#### Активация пользователей вручную

Для того, чтобы активировать пользователя необходимо перейти в раздел пользователей, и открыть УЗ необходимого пользователя. В открытой форме пользователя переключить значение атрибута «**Активен**», в области «**Статус**» на значение «**ВКЛ**». И сохранить нажатием на кнопку «**Сохранить**».

После сохранения запись в атрибуте «**Причина** **блокировки**» очистится. Пользователь будет активным.

###  Блокирование пользователей вручную

Для того чтобы заблокировать пользователя, для блокировки доступа в Prisma и/или подключенную ИС, необходимо в открытой форме пользователя переключить значение атрибута «**Активен**», в поле «**Статус**», на значение «**ВЫКЛ**». После переключения на форме отобразится атрибут «Причина блокировки», который необходимо заполнить причиной блокировки.

###  Блокировка\активация учетной записи при превышении максимального количества неудачных попыток входа

Параметры защиты безопасности для Prisma задаются на вкладке «Защита безопасности». Защита происходит путем определения атак методом подбора паролей. Для того, чтобы настроить ограничение количества неуспешных попыток входа в Prisma и/или в подключенные ИС, необходимо перейти на вкладку «Защита безопасности».

На открывшейся странице перевести в активное состояние переключатель «Включено», который включает или отключает защиту.

#### Блокирование пользователей при отсутствии активностей

Учетные записи, которые не используются в течение заданного времени, автоматически блокируются, когда срок их последнего использования превысит указанный в параметре «Кол-во дней до блокировки». Параметр указывается на странице Настроек пользователей (Пользователи->Настройки).

#### Уведомление пользователей о предстоящей блокировке

Пользователи, которые бездействовали определенный период, и у которых до блокировки остается указанное время (дней) - таким пользователям отправляется уведомление о предстоящей блокировке.

#### Самостоятельная блокировка пользователя

Запрос на самостоятельную блокировку своей УЗ происходит через API. Запрос могут выполнить только аутентифицированные пользователи.

### Удаление пользователей

Ручное удаление пользователей в Prisma запрещено.

Удаление заблокированных пользователей происходит автоматически по истечению трех лет хранения заблокированных УЗ.

Временные УЗ удаляются автоматически, по истечению срока активности, и, если нет записей в журналах аудита.

###  Настройки входа

Prisma позволяет включить или выключить определенные общие функции входа, а именно:

* возможность самостоятельной регистрации пользователей - на странице входа добавляется ссылка на форму регистрации. Процесс регистрации проходит по настроенному сценарию аутентификации;
* использовать e-mail как логин - при включении данной функции, при самостоятельной регистрации, пользователю не будет доступно поле «Логин» для заполнения. При сохранении данное поле заполнится значением в поле e-mail;
* иные функции входа.

### Изменение логина после создания учетной записи (УЗ)

Изменение логина после создания учетной записи может быть только в той Области ИС, где включена данная функция.

### Работа с паролями

#### Установка и смена паролей

Установка первоначального пароля Администратором, а также последующая смена пароля, проводится одними и теми же действиями.
Для смены пароля пользователя необходимо перейти во вкладку «Учетные данные карточки пользователя».

Если пароль не соответствует парольным политикам, сохранение пароля не произойдет, а Prisma сообщит пользователю, что пароль не соответствует парольным политикам.

#### Управление парольными политиками

Установка проверок для сложности пароля задается с помощью «Политики паролей».

#### Сброс учетных данных пользователя

Для сброса учетных данных пользователю необходимо перейти на страницу сопоставлений аутентификации перейти в раздел Аутентификация и в открывшейся рабочей панели ниже перейти на вкладку «Сопоставления».

## Управление доступом

### Проверка наличия и выдача требуемых прав пользователям

Проверку наличия и выдачу требуемых пользовательских прав (ролей) можно осуществить 3 способами:

1. С помощью раздела Роли можно посмотреть для каких пользователей назначена та или иная роль;
2. В карточке выбранного пользователя можно посмотреть назначенные роли, роли области ИС и роли клиентов, присвоенные пользователю;
3. С помощью раздела Группы можно посмотреть какие роли присвоены пользователям, добавленным в выбранную группу.

### Управление областями видимости

#### Просмотр списка областей видимости

Для просмотра списка Областей видимости необходимо открыть раздел областей видимости, который находится в меню слева, в категории Пользователи. После открытия раздела, в нем отобразится список всех доступных ОВ.

#### Создание областей видимости

Для создания области видимости необходимо в открывшемся разделе нажать на кнопку «+Область видимости».

#### Редактирование областей видимости

Для того чтобы отредактировать определенную область видимости, необходимо выбрать ОВ и нажать на название этой ОВ, либо нажать на кнопку меню в виде трех точек справа и далее нажать **Редактировать**.

#####  Изменение композитной ОВ

Для изменения композитности ОВ необходимо в меню редактирования переключить тумблер «Композитная область видимости». Далее, если вы хотите сделать композитную ОВ, необходимо выбрать ОВ, которые будут входить в состав композитной. После внесения изменений для их сохранения, необходимо нажать на кнопку **Сохранить**.

#### Удаление областей видимости

Для того чтобы удалить определенную Область видимости, необходимо выбрать ОВ и нажать на кнопку меню в виде трех точек справа и далее нажать **Удалить**.

Область видимости не удалится, если:

* удаляемая ОВ связана с доменами (прямая связь домена именно с этой ОВ);
* удаляемая ОВ входит в состав композитных ОВ и при ее удалении измененная композитная ОВ потеряет свою «уникальность» и станет дубликатом другой композитной ОВ.

### Управление ролями

#### Назначение пользователю роли через карточку определенной роли

Один из вариантов назначения ролей Области ИС или доступных клиентских ролей - через карточку самой роли.

#### Просмотр списка пользователей включенных в роль

Для того чтобы просмотреть список пользователей, которым присвоена определенная роль, необходимо:

1. В разделе «Роли» выбрать определенную роль;
2. Перейти на вкладку «Пользователи» определенной роли;
3. На открывшейся вкладке отобразятся все пользователи, которым присвоена выбранная роль.

#### Просмотр списка ролей Области ИС или Prisma

Для того, чтобы просмотреть список ролей определенной Области ИС, ролей клиентов определенной Области ИС или Мастер Области ИС необходимо в меню выбрать пункт «**Роли**» в требуемой Области ИС (в каждой Области ИС свой раздел «Роли»).

#### Редактирование роли

Чтобы отредактировать клиентскую роль необходимо:

1. Перейти в раздел «Роли». В списке отобразятся роли, доступные текущему пользователю.
2. Далее нужно определить необходимую роль.
3. На строке с этой ролью выбрать действие «**Редактировать**» через нажатие на значок трех вертикальных точек в правой части экрана.

Пока у роли назначена хоть одна роль, признак «Композитная» не доступен для редактирования. Данный признак автоматически снимается при удалении всех назначенных ролей из списка.

#### Роли по умолчанию

Для Клиентов Prisma существуют роли по умолчанию, которые им можно сразу назначить. Список назначенных клиентам ролей по умолчанию можно посмотреть, перейдя в раздел **Роли**, во вкладку **Роли по умолчанию**.

В отображенном списке ролей по умолчанию мы видим наименование роли и клиента, которому эта роль назначена. Нажав на кнопку «Фильтр» можно отфильтровать список ролей по умолчанию по определенным ролям и\или клиентам.

#### Создание композитных ролей

Любую роль на уровне области или клиента можно превратить в композитную (составную) роль. *Композитная роль —* это роль, которая имеет один или несколько дополнительных функций, связанных с ней.

Когда композитная роль сопоставлена пользователю, пользователь также получает роли, связанные с этой ролью. Это наследование является рекурсивным, поэтому любая композиция композитов также наследуется.

Чтобы превратить обычную роль в композитную, перейдите на страницу деталей роли и включите переключатель «Композитные роли».

#### Создание роли Клиента

Для создания новой роли Области ИС необходимо перейти в раздел «Роли» и нажать на кнопку «**+ Роль**».

#### Удаление роли

Чтобы удалить роль Области ИС или клиентскую роль, необходимо перейти в [раздел «Роли»](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=128694358). В списке отобразятся роли, доступные текущему пользователю.

При удалении роли, так же удаляются все созданные с ней связи.

#### Управление атрибутами ролей

Для управления атрибутами определенной роли, требуется перейти в раздел роли и открыть нужную роль, выбрав пункт редактировать.

###  Управление группами пользователей

#### Просмотр групп

Для просмотра списка групп необходимо перейти в раздел **Группы.**



Рисунок 6 Группы пользователей

#### Создание группы

Группы в Prisma позволяют управлять общим набором атрибутов и сопоставлений ролей для набора пользователей. Пользователи могут входить в одну или более групп или не входить вовсе. Пользователи наследуют сопоставления ролей, назначенные каждой группе.

Для того, чтобы создать группу, необходимо выбрать родительскую группу и выбрать пункт «Создать группу» в контекстном меню или нажать на кнопку «+ Группа».

#### Редактирование группы

##### Редактирование определенной группы

Для того чтобы редактировать Группу, необходимо навести курсор на необходимую группу и открыть контекстное меню. В контекстном меню выбрать действие «Редактировать».

##### Изменение Иерархии групп через контекстное меню

Для того, чтобы изменить родительскую группу определенной дочерней группе или дочерней группе убрать родительскую, необходимо открыть контекстное меню группы и выбрать действие «Вырезать».

После этого выбрать группу, которая будет родительской (или общий элемент, в случае если группа перемещается на самый верхний уровень) и в контекстном меню выбрать действие «Вставить». Группа будет перенесена.

#### Удаление группы

Для удаления групп необходимо перейти в раздел «Группы», выделить требуемую группу в дереве групп и нажать кнопку «**Удалить**» в контекстном меню.

После чего запись будет удалена из списка групп. Если в родительской группе были дочерние группы, то они также будут удалены.

#### Атрибуты групп

Атрибуты групп предназначены для хранения свободной информации о группах пользователей.

Для управления атрибутами определенной группы, требуется перейти в раздел **Группы** и открыть карточку требуемой группы, выбрав действие «Редактировать» в контекстном меню.

##### Добавление и удаление пользователя из группы

Добавление и исключение пользователей из групп доступно в следующих разделах Prisma:

* в карточке пользователя, во вкладке «Группы»
* или в карточке определенной группы, во вкладке «Пользователи»

#### Назначение ролей группам

Как и пользователям, группам можно назначать роли. Это предназначено для упрощения назначения ролей пользователям, если предусмотрено большое количество ролей, которые необходимо назначить пользователям.

#### Управление группами по умолчанию

Для исключения рутинной работы по назначению групп новым пользователям, в Prisma предусматривается автоматическое назначение групп, которые указаны как группы по умолчанию. При создании пользователей они автоматически включаются во все группы, которые указаны как группы по умолчанию.

#####  Добавление групп в список групп по умолчанию

Для указания групп, которые будут назначаться всем пользователям, при их создании, Администратор Области ИС переходит в раздел «Группы» и открывает вкладку «Группы по умолчанию».

На открывшейся странице отображаются все группы, которые назначаются всем пользователям, при их создании.
Далее необходимо нажать на кнопку «+Группа». После нажатия, в открывшейся форме, требуется выбрать группу, которая будет назначаться по умолчанию и нажать кнопку «Добавить».

Исключение групп из списка групп по умолчанию происходит в этом же разделе.

### Переход к настройкам авторизации клиента

Для перехода на страницу настроек авторизации клиента сначала необходимо в настройках выбранного клиента:

1. Выбрать тип доступа «Confidentional» в раскрывающемся списке поля «Тип доступа»;

2. Далее в появившихся ниже переключателях нажать на переключатель «Авторизация включена».

3. Сохранить или отменить внесенные изменения с помощью кнопок в нижней части окна.

После выполнения этих действий в рабочей панели сверху появится вкладка «Авторизация».

###  Управление разрешениями

#### Управление разрешениями пользователей

Для просмотра доступных разрешений пользователей, необходимо:

1. Перейти в раздел «Пользователи»;
2. На рабочей панели сверху перейти на вкладку «Разрешения».

На открывшейся вкладке отображаются все разрешения, которые доступны пользователям в текущий момент.



Рисунок 7 Список доступных пользовательских разрешений

В верхней части списка есть переключатель «Включить разрешения», который определяет, включены ли подробные разрешения. Отключение переключателя приводит к исключению всех текущих настроенных разрешений.

#### Просмотр разрешений клиентов

Для просмотра доступных разрешений клиентов, пользователю необходимо перейти в раздел «Клиенты» и на рабочей панели сверху перейти на вкладку «Разрешения».

#### Редактирование разрешения клиента

Переход в режим редактирования Разрешения осуществляется 2 способами:

* Нажатием на наименование необходимого Разрешения;
* Переходом к кнопке «Редактировать» после нажатия на значок «Вертикальное многоточие» справа от наименования Разрешения.

#### Управление разрешениями групп

Для просмотра разрешений определенной группы пользователю необходимо:

1. Перейти в раздел «Группы» на рабочей панели в левой части экрана.
2. Далее необходимо:
	* Либо [создать новую группу](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=118143675);
	* Либо через наведение курсора на нужную группу нажать на кнопку «[Редактировать](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=118143686)«. Кнопка появляется при наведении курсора на значок трех точек, справа от названия группы.
3. По умолчанию пользователь попадает в раздел «Настройки» выбранной группы;
4. В появившейся рабочей панели необходимо перейти на вкладку «Разрешения», правее от вкладки «Настройки».

#### Управление разрешениями относительно выбранной роли

Для перехода в раздел разрешений ролей пользователю необходимо:

1. [В списке ролей](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=131054691) выбрать необходимую роль;
2. В появившейся рабочей панели сверху перейти на вкладку «Разрешения».

### Настройки авторизации клиента

На данной странице есть поля с выпадающими списками:

* Режим применения политик - определяет, каким образом политики применяются при оценке запросов на авторизацию.
* Стратегия решения (cтратегия принятия решения) - определяет, как оцениваются разрешения и как принимается окончательное решение.

## Управление сессиями

###  Просмотр, фильтрация и сортировка списка активных сессий для ИС или ее части

Когда пользователь входит в Область ИС, подключенную ИС или Prisma для него открывается сеанс доступа, который позволяет перемещаться по доступным ИС без повторной аутентификации.

Для того чтобы просмотреть список активных сеансов необходимо открыть пункт меню «Сеансы».

###  Просмотр списка оффлайн сессий пользователей в Области ИС

В определенных случаях взаимодействия пользователей и приложений, которые подключены к Prisma, могут возникнуть ситуации, когда требуется выполнить определенные действия от имени пользователя, но без его участия. В таких ситуациях пользователю открывается Оффлайн сессия. Отличия ее от активной сессии в том, что для получения ее требуются отдельные разрешения от пользователя и срок жизни данной сессии дольше обычного.

Для того чтобы просмотреть список оффлайн сессий необходимо открыть пункт меню «Сеансы» и перейти во вкладку «Оффлайн сессии».

###  Ограничение числа параллельных сессий

Чтобы задать настройки при превышении пользователем допустимого количества параллельных сессий необходимо:

1. Перейти в раздел «Аутентификация»;
2. На открывшейся странице выбрать необходимый сценарий входа;
3. В меню действий на строке «User Session Count Limiter» необходимо выбрать «Конфигурация».

###  Завершение сессий администратором подключенной ИС

Для завершения сессий пользователей необходимо перейти в раздел «Сессии», вкладка «Онлайн сессии». При необходимости отфильтровать список сессий. В контекстном меню требуемой сессии выбрать пункт «Завершить сессию».

###  Автоматическое принудительное закрытие сессий по таймауту

Для предотвращения получения доступа третьими лицами, Prisma, согласно установкам в настройках, автоматически прерывает активные сессии после времени бездействия.

Если сессия отсутствует, либо просрочена, то при попытке выполнить какое-либо действие в системе, пользователь пересылается на страницу аутентификации с пустыми строками логин, пароль.

###  Завершение собственных сессий субъектом доступа

Для закрытия своего сеанса доступа, внутреннему пользователю необходимо нажать на кнопку «Выход». Даная кнопка доступна выводится на экран после открытия «Меню пользователя» на каждой странице Prisma.

## Журналирование и контроль изменений

###  Настройки регистрации событий безопасности

Для настройки параметров журналирования необходимо открыть раздел **События** и перейти во вкладку **Настройки.** Откроются три дополнительные вкладки настроек журналирования событий, включающие в себя:

1. Общие настройки.

2. Журнал входа.

3. Журнал администратора.

### Журналирование событий входа и выхода пользователей

Для просмотра событий попыток входа, входа и выхода необходимо открыть раздел «События» и открыть вкладку «События входа».

На данной вкладке отображаются все выбранные в параметрах события входа\выхода и попыток входа. События отображаются постранично. Количество записей, отображаемых на данной странице, регулируется пользователем (доступные значения 5, 10, 20, 50, 100).

###  Журналирование действий администраторов

На данной странице отображаются все доступные события (согласно разрешениям) Prisma или Области ИС с подключенными ИС. В случае использования сервиса регистрации событий Подключенной ИС, они так же отображаются на данной странице.

###  Ограничение времени хранения событий безопасности

Для настроек ограничения времени хранения событий безопасности пользователю необходимо:

1. Перейти в раздел События на рабочей панели слева;
2. Далее выбрать подраздел Настройки в открывшейся панели в верхней части экрана;
3. И ниже выбрать подраздел Журнал администратора.

### Очистка событий безопасности вручную

Для ручной очистки событий безопасности пользователю необходимо:

1. Перейти в раздел События на рабочей панели слева;
2. Далее выбрать подраздел Настройки в открывшейся панели в верхней части экрана;
3. Ниже выбрать подраздел:
* Либо журнал администратора;
* Либо журнал входа.

### Трансляция событий в syslog

Для передачи событий на сервер syslog требуется внести изменения в конфигурационный файл.

###  Уведомления при критических сбоях в механизмах сбора информации

События безопасности записываются во внутренние журналы Prisma согласно настроенных параметров.

###  Автоматическая рассылка уведомлений об изменении администраторами прав пользователей

Для автоматической рассылки уведомлений об изменении администраторами прав пользователей необходимо:

1. Перейти в раздел Настройки;
2. Далее в подразделе e-mail нужно произвести настройку SMTP-сервера (подробнее описано далее в разделе «Настройка SMTP-сервера»).

### Рассылка уведомлений при заполнении объема памяти

Для выполнения условия в Области ИС должно быть установлено «Ограничение размера журнала событий», а также пользователь должен зайти в Мастер Область ИС.

### Рассылка уведомлений о критическом сбое

Чтобы своевременно предпринять меры по устранению сбоя, Prisma отправляет пользователям и администраторам сообщения на электронную почту о критических сбоях в механизмах регистрации информации.

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

|  |  |
| --- | --- |
| **АРМ** | Автоматизированное рабочее место |
| **БД** | База данных |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ОВ** | Область видимости |
| **ОС** | Операционная система |
| **ОЦЛ** | Обеспечение целостности информационной системы и информации |
| **ПО** | Программное обеспечение |
| **РСБ** | Регистрация событий безопасности |
| **СЗИ** | Средство защиты информации |
| **СУБД** | Система управления базами данных |
| **ТУ** | Технические условия |
| **УПД** | Управление доступом субъектов доступа к объектам доступа |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |
| **Prisma** | Professional Identity Security Manager |
| **SSO** | Single sign-on |
| **URL** | Uniform Resource Locator |

# ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

**Администратор Prisma** - лицо, ответственное за функционирование Prisma, в установленном штатном режиме работы, согласно правилам разграничения доступа.

**Администратор ИБ подключенной ИС** - лицо, ответственное за функционирование информационной системы, в установленном штатном режиме работы, согласно правилам разграничения доступа.

**Внутренние событие безопасности** - события безопасности, которые происходят в результате управления субъектами и объектами доступа Prisma, конфигурацией Prisma, управлением объектами и субъектами доступа информационной системы и конфигурации ИС через интерфейс Prisma.

**Внешнее событие безопасности** - события безопасности, которые происходят в следствии отправки запросов подключенной информационной системой в Prisma, связанных с получением разрешения на выполнение действия в подключенной информационной системе.

**Временная учетная запись** - учетная запись, у которой ограничено время действия (жизни).

**Информационная система. Подключаемая информационная система** - информационная система, использующая Prisma для выполнения функций безопасности

**Клиент** - определенная подсистема подключенной информационной системы, которая использует функции Prisma

**Событие безопасности** - системное событие, которое возникает в результате выполнения функций и при выполнении определенных условий, связанных с работой Prisma.

**Субъект доступа** - пользователь, процесс, выполняющие действия над объектами доступа и действия которых регламентируются правилами разграничения доступа

**Single sign-on** — это средство аутентификации, позволяющее пользователям осуществлять доступ к нескольким приложениям с помощью одного набора учетных данных.